

LINEAR REPRESENTATION OF ABEL-GRASSMANN GROUPS

DAVID STANOVSKÝ

ABSTRACT. We describe a linear representation for Abel-Grassmann groups. As a consequence, we obtain or improve many previous results. In particular, enumeration of Abel-Grassmann groups up to isomorphism is obtained for orders < 512 .

1. INTRODUCTION

By a *groupoid* we mean an algebraic structure (G, \cdot) with a single binary operation. A groupoid is called *Abel-Grassmann* (shortly, *AG-groupoid*) if it satisfies the identity

$$(a \cdot b) \cdot c = (c \cdot b) \cdot a$$

for every $a, b, c \in G$. Groupoids satisfying an additional identity

$$a \cdot (b \cdot c) = b \cdot (a \cdot c)$$

for every $a, b, c \in G$ are called *AG^{**}-groupoids*. In a number of recent papers, e.g., [3, 4, 10, 12, 13], it has been demonstrated that the theory of AG^{**}-groupoids has a strong parallel to the theory of commutative semigroups, and this phenomenon seems to be the main motivation for their study. Some indication that this is not a coincidence can be found in [1] and [7, Chapter 3], see our Section 4 for comments.

As a proof of concept, in this paper, we focus on a particular subclass of AG^{**}-groupoids, called *Abel-Grassmann groups* (shortly, *AG-groups*)¹. They are defined as groupoids (G, \cdot) satisfying three axioms similar to the axioms of groups:

- the Abel-Grassmann identity $(a \cdot b) \cdot c = (c \cdot b) \cdot a$ holds for every $a, b, c \in G$;
- there exists a *left unit* e , i.e., an element satisfying $e \cdot a = a$ for every $a \in G$;
- for every $a \in G$ there exists a unique a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

For example, every abelian group A is an AG-group, and also $(A, *)$ with $a * b = b - a$ is an AG-group. We believe [8, 11, 14, 15, 16] is the complete list of references to AG-groups (in earlier papers, they were called LA-groups).

It has been noticed (e.g., in [15]) that every AG-groupoid is *medial*, i.e., the identity $(ab)(cd) = (ac)(bd)$ holds for every a, b, c, d , and that every AG^{**}-groupoid is *paramedial*, i.e., the identity $(ab)(cd) = (db)(ca)$ holds for every a, b, c, d (paramediality is somewhat lesser known, see [2] for an account on paramediality). Also, every AG-group is an AG^{**}-groupoid. Importantly, AG-groups are *quasigroups* (latin squares), i.e., they possess unique left and right division. While this fact is implicit in [15], we could not find a complete proof anywhere.

The main result of our paper is the following characterization of Abel-Grassmann groups.

Theorem 1.1. *The following conditions are equivalent for a groupoid (G, \cdot) :*

Date: December 1, 2014.

2010 Mathematics Subject Classification. 20N05, 20N02.

Key words and phrases. Abel-Grassmann group, AG^{**}-groupoid, paramedial quasigroup, affine representation.

Partly supported by the GAČR grant 13-01832S.

¹In my opinion, the choice of name is somewhat unlucky, since these structures are not groups. But let me keep the established terminology.

- (1) (G, \cdot) is an AG-group.
- (2) (G, \cdot) is an AG^{**} -quasigroup.
- (3) (G, \cdot) is a paramedial quasigroup with a left unit.
- (4) There exists an abelian group $(G, +)$ and its automorphism φ satisfying $\varphi^2 = id$ such that $a \cdot b = \varphi(a) + b$ for every $a, b \in G$.

In particular, condition (4) provides a complete classification of AG-groups in terms of abelian groups and their involutory automorphisms. (For the examples above, take $\varphi(a) = a$, and $\varphi(a) = -a$, respectively.) It can also be interpreted as a *linear representation* for every AG-group over a module over the ring $\mathbb{Z}[x]/(x^2 - 1)$. This fact has a number of consequences and easily explains virtually all the results on AG-groups in the papers listed above.

Let us note that Theorem 1.1 is not surprising. By an *affine representation* of a quasigroup (G, \cdot) we mean an abelian group $(G, +)$, its automorphisms φ, ψ , and $c \in G$ such that

$$a \cdot b = \varphi(a) + \psi(b) + c$$

for every $a, b \in G$. Since AG-groups are medial quasigroups, the Toyoda-Bruck representation theorem [17] applies, and we obtain an affine representation with an additional condition that $\varphi\psi = \psi\varphi$. Since AG-groups are paramedial quasigroups, the Kepka-Němec representation theorem [9] applies, and we obtain an affine representation with an additional condition that $\varphi^2 = \psi^2$. Existence of a left unit then implies $\varphi^2 = \psi = id$. Nevertheless, in our paper we present a direct proof, which allows a simpler (linear, with $c = 0$) representation, and a bit more.

In fact, we prove a stronger version of Theorem 1.1 in Section 2: there is a *term equivalence* between the varieties of AG-groups, AG^{**} -quasigroups, paramedial quasigroups with a left unit, and modules over the ring $\mathbb{Z}[x]/(x^2 - 1)$. It means, the four varieties are essentially identical, up to choice of the basic operations. Consequently, all properties determined by term operations translate straightforwardly from one setting to another. For example, in modules, congruences (i.e., kernels of homomorphisms) are determined by subalgebras, thus the same correspondence exists in all four settings. At the end of Section 2, we make a comparison to a correspondence developed in [14].

In section 3, we enumerate AG-groups up to isomorphism, for every size < 512 , and every size $p_1^{d_1} \cdots p_k^{d_k}$ with all $d_i \leq 2$. This dramatically improves results of [16], where enumeration was given up to size 11.

In section 4, we present a few remarks towards extending the results to other classes of AG^{**} -groupoids.

We will use the following notation to reduce the number of parentheses: for instance, $ab \cdot cd$ will stand for $(a \cdot b) \cdot (c \cdot d)$, and similarly for other expressions. All identities are meant to be universally quantified, unless stated otherwise.

2. EQUIVALENCE OF THE FOUR CONCEPTS

We start with a few observations. Most of them can be traced in [14, 15].

Lemma 2.1.

- (1) An AG^{**} -quasigroup is paramedial, the mapping $f(a) = a/a$ is constant, and $e = a/a$ is a left unit.
- (2) A paramedial groupoid with a left unit is an AG-groupoid.
- (3) An AG-groupoid with a left unit is an AG^{**} -groupoid.

Proof. (1) For paramediality, calculate

$$ab \cdot cd = c \cdot (ab \cdot d) = c \cdot (db \cdot a) = db \cdot ca.$$

To prove that $a/a = b/b$ for every a, b , calculate

$$(a/a) \cdot b = (a/a) \cdot ((b/a)a) = (b/a) \cdot ((a/a)a) = (b/a) \cdot a = b$$

and divide by b from right. In particular, we see that $e = a/a$ is a left unit.

(2) Let e be a left unit. Then

$$ab \cdot c = ab \cdot ec = cb \cdot ea = cb \cdot a.$$

(3) Let e be a left unit again. Then

$$a \cdot bc = ea \cdot bc = (bc \cdot a)e = (ac \cdot b)e = eb \cdot ac = b \cdot ac.$$

□

As an immediate corollary, we obtain the equivalence (2) \Leftrightarrow (3) of Theorem 1.1.

From universal algebraic perspective, it is convenient to work with varieties. Therefore, we have to introduce symbols for all operations we want to perform. We will consider the following varieties.

The variety of AG-groups is the variety of algebras $(G, \cdot, ^{-1}, e)$ satisfying the identities

$$ab \cdot c = cb \cdot a, \quad aa^{-1} = a^{-1}a = e, \quad ea = a.$$

The variety of AG^{**} -quasigroups is the variety of algebras $(G, \cdot, /, \backslash)$ satisfying the identities

$$ab \cdot c = cb \cdot a, \quad a \cdot bc = b \cdot ac, \quad a \cdot (a \backslash b) = a \backslash (a \cdot b) = (b/a) \cdot a = (b \cdot a)/a = b.$$

The variety of $\mathbb{Z}[x]/(x^2 - 1)$ -modules is the variety of algebras $(G, +, -, 0, \varphi)$ such that $(G, +, -, 0)$ is an abelian group and

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(\varphi(a)) = a.$$

(Clearly, the action of the ring $\mathbb{Z}[x]/(x^2 - 1)$ is given by the action of the monomial x , which in turn acts as an involutory automorphism φ .)

Theorem 2.2. *The varieties of AG-groups, AG^{**} -quasigroups and $\mathbb{Z}[x]/(x^2 - 1)$ -modules are term equivalent.*

Proof. First, we translate AG-groups to AG^{**} -quasigroups. The identity $a \cdot bc = b \cdot ac$ was proved in Lemma 2.1(3). It remains to show that AG-groups have term definable unique left and right division. We start with uniqueness of right division. If $xa = b$, then $xa \cdot a^{-1} = ba^{-1}$, and since $xa \cdot a^{-1} = a^{-1}a \cdot x = ex = x$, we necessarily have $x = ba^{-1}$. Now it is easy to check that this really is a solution: $ba^{-1} \cdot a = aa^{-1} \cdot b = eb = b$. Hence, we have a term definable unique right division, namely

$$b/a = ba^{-1}$$

(see also [14, Lemma 2.3] for this observation). Now we solve $ax = b$. Since $ax = ea \cdot x = xa \cdot e$, we have $ax = b$ iff $xa \cdot e = b$ iff $x = (b/e)/a = be^{-1} \cdot a^{-1} = be \cdot a^{-1}$. Hence, we have a term definable unique left division, namely

$$a \backslash b = be \cdot a^{-1}.$$

In the second step, we translate AG^{**} -quasigroups to $\mathbb{Z}[x]/(x^2 - 1)$ -modules. First recall that $e = a/a$ is a term definable left unit (independent of the choice of a), see Lemma 2.1(1). Let

$$a + b = ae \cdot b, \quad -a = (ae) \backslash e, \quad 0 = e, \quad \varphi(a) = ae$$

(the definition of the group operations can be found in [1, Theorem 2.9] and [14, Theorem 2.4]). To check $(G, +, -, 0)$ is an abelian group, calculate $a + b = ae \cdot b = be \cdot a = b + a$, $0 + a = ee \cdot a = ea = a$, $a + (-a) = ae \cdot (ae) \backslash e = e = 0$, and

$$a + (b + c) = ae \cdot (be \cdot c) = ae \cdot (ce \cdot b) = ce \cdot (ae \cdot b) = (ae \cdot b)e \cdot c = (a + b) + c.$$

To check that φ is an involutory automorphism, calculate $\varphi^2(a) = ae \cdot e = ee \cdot a = ea = a$, and finally,

$$\varphi(a + b) = (ae \cdot b)e = eb \cdot ae = b \cdot ae = (be \cdot e) \cdot ae = \varphi(b) + \varphi(a) = \varphi(a) + \varphi(b).$$

In the last step, we translate $\mathbb{Z}[x]/(x^2 - 1)$ -modules to AG-groups. Let

$$a \cdot b = \varphi(a) + b, \quad a^{-1} = \varphi(-a), \quad e = 0.$$

For the Abel-Grassman identity,

$$ab \cdot c = \varphi(\varphi(a) + b) + c = a + \varphi(b) + c = \varphi(\varphi(c) + b) + a = cb \cdot a,$$

the inverse properties follow from

$$a \cdot a^{-1} = \varphi(a) + \varphi(-a) = 0 = e, \quad a^{-1} \cdot a = \varphi(\varphi(-a)) + a = 0 = e,$$

and e is a left unit since $ea = \varphi(0) + a = a$. \square

Theorem 1.1 is an immediate consequence of Lemma 2.1 and Theorem 2.2. However, Theorem 2.2 implies a stronger connection between the four concepts: any property or feature that only depends on term operations is equivalent in all four settings (for instance, subalgebras, congruences, homomorphisms, and their properties). In particular, it allows to translate many properties of modules to the AG-group setting.

Naturally, a subset H of an AG-group G is a *sub-AG-group* if $a \cdot b \in H$, $a^{-1} \in H$ and $e \in H$ for every $a, b \in H$. Using Theorem 2.2, H is a sub-AG-group if and only if H is a submodule of the corresponding $\mathbb{Z}[x]/(x^2 - 1)$ -module, i.e., if and only if $a + b = ae \cdot b \in H$, $-a = (ae) \setminus e = ee \cdot (ae)^{-1} = (ae)^{-1} = a^{-1}e \in H$, $0 = e \in H$ and $\varphi(a) = ae \in H$ for every $a, b \in H$. Hence, for example, all finite AG-groups satisfy the *Lagrange property* (if B is a subalgebra of A , then $|B|$ divides $|A|$), because all finite modules do (see [11] for a different argument).

Similarly for congruences. In modules, subalgebras and ideals (i.e., kernels of homomorphisms) is the same thing. Therefore, so it is in AG-groups. Every congruence α of an AG-group G is uniquely determined by its block e/α containing the left unit e , and this block forms a subalgebra, i.e., a sub-AG-group. Conversely, every sub-AG-group H of G determines a unique congruence defined by $a \sim b$ iff $a - b \in H$. Since $a - b = a + (-b) = ae \cdot b^{-1}e = b^{-1}a$ (using paramediality), a sub-AG-group H determines the congruence defined by

$$a \sim b \iff b^{-1}a \in H.$$

In particular, all AG-groups have *ideal-determined congruences* (congruences are uniquely determined by their block containing the left unit), and thus are *congruence permutable* ($\alpha \vee \beta = \alpha \circ \beta = \beta \circ \alpha$ for any pair of congruences) and thus also *congruence modular* (see [6] for more information on ideal-determined varieties).

Let us note that a recent paper by Protić [14, Theorem 3.4] contains a more complicated description of the correspondence between subalgebras and congruences. He considers *normal sub-AG-groups* as subsets $H \subseteq G$ closed with respect to all three AG-group operations and such that $u \cdot au^{-1} \in H$ for every $a \in H$ and $u \in G$. However, it is easy to see that every sub-AG-group is normal in Protić's sense: we have $u \cdot au^{-1} = a \cdot uu^{-1} = ae \in H$, because both $a, e \in H$.

3. ENUMERATION

In [16], the enumeration of AG-groups of size ≤ 11 was presented, using a brute force search with a few non-trivial symmetry-breaking heuristics. Here we show how the algebraic theory can be used to obtain enumeration of much larger scale.

Let $(G, +)$ be an abelian group and φ its involutory automorphism. The AG-group (G, \cdot) with $x \cdot y = \varphi(x) + y$ will be denoted $\text{AGG}(G, \varphi)$. Theorem 1.1 says that every AG-group admits such a representation. The first step in our enumeration is an isomorphism theorem.

Proposition 3.1. *Let G, H be two abelian groups and φ, ψ their involutory automorphisms, respectively. A mapping $f : G \rightarrow H$ is an isomorphism $\text{AGG}(G, \varphi) \simeq \text{AGG}(H, \psi)$ if and only if f is a group isomorphism $G \simeq H$ and $\psi = f\varphi f^{-1}$.*

d	1	2	3	4	5	6	7	8
$a(2^d)$	1	4	10	29	69	187	449	1141
$a(3^d)$	2	5	10	20	36	65		
$a(5^d)$	2	5	10	20				
$a(7^d)$	2	5	10					
$a(p^d)$	2	5						

TABLE 1. Enumeration of AG-groups.

Proof. It follows from Theorem 2.2 that a mapping $f : G \rightarrow H$ is a homomorphism with respect to AG-group operations, i.e., $f(a \cdot b) = f(a) \cdot f(b)$, $f(a^{-1}) = f(a)^{-1}$ and $f(e) = e$, if and only if it is a homomorphism with respect to the corresponding $\mathbb{Z}[x]/(x^2 - 1)$ -module operations, i.e., $f(a + b) = f(a) + f(b)$ and $f(\varphi(a)) = \psi(f(a))$. The statement follows immediately. \square

Let $a(n)$ denote the number of isomorphism classes of AG-groups with n elements. According to Proposition 3.1, $a(n)$ equals the sum of the numbers of involutory automorphisms up to conjugacy, where the sum runs over all abelian groups of order n up to isomorphism. If m and n are coprime, the classification of finite abelian groups implies that $a(mn) = a(m)a(n)$. Therefore, we can focus on $a(p^d)$ for prime powers p^d . We start with the enumeration of AG-groups of prime order or prime squared order.

Proposition 3.2. *If $p > 2$ is a prime, then $a(p) = 2$ and $a(p^2) = 5$. For $p = 2$, $a(2) = 1$ and $a(4) = 4$.*

Proof. First consider the prime size. In this case any AG-group is isomorphic to $\text{AGG}(\mathbb{Z}_p, k)$ where $k \in \mathbb{Z}_p^*$ satisfies $k^2 \equiv 1 \pmod{p}$. Since \mathbb{Z}_p^* is cyclic, there is only one element of order 2, hence the only solutions are $k = 1$ and $k = p - 1$. If $p = 2$, this is only one solution.

For prime squared, there are two possibilities. If $G = \mathbb{Z}_{p^2}$, we proceed similarly. If $k^2 \equiv 1 \pmod{p^2}$, that is, $p^2 \mid k^2 - 1 = (k - 1)(k + 1)$, then either $k = 1$, or $k = p^2 - 1$, or p divides both $k - 1$, $k + 1$, which is impossible unless $p = 2$. In any case, we obtain two solutions.

Let $G = (\mathbb{Z}_p)^2$. Its automorphism group is $GL(2, \mathbb{F}_p)$, hence we need to determine the number of conjugacy classes of matrices A satisfying $A^2 = I$. Since the polynomial $f = x^2 - 1$ splits over \mathbb{F}_p , such matrices are determined by their Jordan normal form. Now, the key observation is that if a matrix A satisfies $f(A) = 0$, then every eigenvalue of A is a root of f . Hence, for $p = 2$, there are two possible Jordan forms

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Both matrices satisfy $A^2 = I$, hence $a(4) = 2 + 2 = 4$. For $p > 2$, there are five possible Jordan forms

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

The former three matrices satisfy $A^2 = I$, while the latter two matrices do not. Hence $a(p^2) = 2 + 3 = 5$. \square

Further values of $a(p^d)$ can be evaluated in GAP [5] by a straightforward calculation using Proposition 3.1. The values are summarized in Table 1.

4. BEYOND QUASIGROUPS?

Theorem 1.1 translates all questions about AG-groups into questions about abelian groups and their involutory automorphisms (or, about $\mathbb{Z}[x]/(x^2 - 1)$ -modules), and explains why properties of

AG-groups resemble those of abelian groups — recall the comment at the end of the first paragraph of the paper. (It also shows that the claim in [15] that AG-groups are “midway between quasigroups and abelian groups” is not quite precise.)

A natural question for further research is, what about other classes of AG^{**} -groupoids? In particular, we have in mind the class of completely inverse AG^{**} -groupoids studied in detail by Dudek and Gigoń [3, 4]. For instance, their characterization of congruences is very similar to the one given in the theory of inverse semigroups. Is there an equivalence with some variety of inverse semigroups with operators? Perhaps, there is a nice semilinear representation, where the semimodule is built over a commutative inverse semigroup.

Some hints can be found in literature. In [7, Section 3] and a few later papers, various kinds of (semi-)linear and (semi-)affine representations of medial groupoids are established. Perhaps some of the ideas can be exploited in the setting of completely inverse AG^{**} -groupoids. See also [1, Theorems 2.7–2.10] for an attempt to establish such a connection.

REFERENCES

- [1] I. Ahmad, M. Rashad, M. Shah, *Constructions of some algebraic structures from each other*. Int. Math. Forum 7, No. 53-56, 2759-2766 (2012).
- [2] J. R. Cho, J. Ježek, T. Kepka, *Paramedial groupoids*. Czech. Math. J. 49, No.2, 277–290 (1999).
- [3] W. Dudek, R. Gigoń, *Congruences on completely inverse AG^{**} -groupoids*, Quasigroups Relat. Syst. 20, No. 2, 203–209 (2012).
- [4] W. Dudek, R. Gigoń, *Completely inverse AG^{**} -groupoids*, Semigroup Forum 87, No. 1, 201–229 (2013).
- [5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.7; 2012*. (<http://www.gap-system.org>)
- [6] H. P. Gumm, A. Ursini, *Ideals in universal algebras*, Algebra Universalis 19 (1984), 45–54.
- [7] J. Ježek, T. Kepka. *Medial groupoids*. Rozprawy ČSAV, Rada mat. a přír. věd 93/2, 1983, 93 pp.
- [8] M. S. Kamran, *Conditions for LA-semigroups to resemble associative structures*, Ph.D. Thesis, Quaid-i-Azam University, Islamabad, 1993.
- [9] P. Němec, *T-quasigroups I*, Acta Univ. Carolin. Math. Phys. 12 (1971), no. 1, 39–49.
- [10] M. Khan, S. Anis, *An analogy of Clifford decomposition theorem for Abel-Grassmann groupoids*. Algebra Colloq. 21 (2014), No. 2, 347-353.
- [11] Q. Mushtaq, M.S. Kamran, *On left almost groups*, Proc. Pak. Acad. of Sciences, 33 (1996), 1–2.
- [12] Q. Mushtaq, M. Khan, *Semilattice decomposition of locally associative AG^{**} -groupoids*, Algebra Colloq. 16 (2009), 17–22.
- [13] P. Protić, *Congruencies on an inverse AG^{**} -groupoid via the natural partial order*. Quasigroups Relat. Syst. 17 (2009), No. 2, 283-290.
- [14] P. Protić, *Some remarks on Abel-Grassmann’s groups*, Quasigroups and Related Systems 20 (2012), 267–274.
- [15] M. Shah, A. Ali, *Some structural properties of AG-groups*. Int. Math. Forum 6 (2011), No. 33-36, 1661-1667.
- [16] M. Shah, C. Grettton, V. Sorge, *Enumerating AG-groups with a study of Smaradache AG-groups*. Int. Math. Forum 6 (2011), No. 61-64, 3079-3086.
- [17] K. Toyoda, *On axioms of linear functions*. Proc. Imp. Acad. Tokyo 17 (1941), 221–227.

DEPARTMENT OF INFORMATION SYSTEMS AND MATHEMATICAL MODELING, INTERNATIONAL IT UNIVERSITY,
MANAS ST. 34, 050040 ALMATY, KAZAKHSTAN

DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND PHYSICS, CHARLES UNIVERSITY, SOKOLOVSKÁ 83,
18675 PRAHA 8, CZECH REPUBLIC

E-mail address: david.stanovsky@gmail.com